

# Cisco Security Response: Cisco IP Phone 7940 DoS Exploit posted on milw0rm.com

Document ID: 68787

<http://www.cisco.com/warp/public/707/cisco-sr-20060113-ip-phones.shtml>

## Revision 1.1

**Last Updated** 2006 January 13 2315 UTC (GMT)

**For Public Release** 2006 January 13 2130 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

[Cisco Response](#)  
[Additional Information](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Cisco Response

This is a response to the Cisco IP Phone DoS exploit posted to <http://www.milw0rm.com/> on January 10, 2006. The exploit sends a SYN flood that will cause affected phones to reload. Although comments within the code suggest that port 80 should be targeted, the vulnerability resides in the IP stack of the device and can be exploited on any port, regardless of whether the phone is listening.

Cisco has introduced changes to the firmware for 7940 and 7960 IP Phones that will reduce the impact of a denial of service attack. Starting with firmware revision 7.1(1), IP phones that are subject to DoS attacks have the capability to perform load control using TCP throttling. Although it may not be possible to maintain normal operation during an attack, the phones will not reload.

The changes mentioned above are documented in Cisco bug ID [CSCef33398](#) ([registered](#) customers only)

This vulnerability was first reported to Cisco by Knud Erik Højgaard; we thank him for making us aware of this issue. We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

## Additional Information

It is important to note that Cisco best practices for IP Telephony include several recommendations that isolate and protect IP phones from many common attacks. For optimum functionality, these devices should be deployed in accordance with those recommendations. For more information, please see:

- Solution Reference Network Designs:  
<http://www.cisco.com/go/srnd/>
- SAFE Blueprint:  
<http://www.cisco.com/go/safe/>

## Revision History

Revision 1.1	<del>2006 January 13</del>	Updated the Cisco Response section.
Revision 1.0	<del>2006 January 13</del>	Initial public release

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 13, 2006

Document ID: 68787

---